DIGITAL AUTHORITARIANISM & THE GLOBAL THREAT TO FREE SPEECH

Congressional-Executive Commission on China
Thursday, April 26, 2018

Representative Christopher Smith
Cochair

China has the world's largest number of internet users as well as the world's most sophisticated and aggressive internet censorship and control regime. The Chinese government, under the leadership of Xi Jinping, views digital controls as necessary for its political stability and control of core digital technologies as necessary for its economic future.

The Chinese government spends $10 billion on maintaining and improving their censorship apparatus. The U.S. government has an annual internet freedom budget of $55 million and Congress still has little idea how this money is spent.

Over the past year or so, Chinese companies were ordered to close websites that hosted discussions on the military, history, and international affairs and crack down on "illegal" VPNs (in response, Apple was forced to remove VPNs from the China App store). New regulations were announced restricting anonymity online and the Chinese government rolled out impressive new censorship technologies, censoring photos in one-to-one WeChat discussions and disrupting WhatsApp.

Beijing has also deployed facial and voice recognition, artificial intelligence, and other surveillance technologies throughout the country, but particularly targeting the Uyghur ethnic minority, where between 500,000 to 1 million Uyghurs have been detained arbitrarily.

The Chinese government and Communist Party's attempts to enforce and export a digital authoritarianism poses a direct threat to Chinese rights defenders and ethnic minorities and poses a direct challenge to the interests of the U.S. and the international community.

The U.S. must recognize that we are engaged in a battle of ideas with a revitalized authoritarianism—online, in the marketplace, and elsewhere—and we need up our "competitive game" to meet the challenge.

The Administration's National Security Strategy says quite clearly that the Chinese government and Communist Party (along with Russia) seek to

> "challenge American power, influence, and interests, attempting to erode American security and prosperity. They are determined to make economies less free and less fair, to grow their militaries, and to control information and data to repress their societies and expand their influence."
>
> [The Chinese government and Communist Party] is using economic inducements and penalties, influence operations, and implied military threats to persuade other states to heed its political and security agenda… China gathers and exploits data on an unrivaled scale and spreads features of its authoritarian system, including corruption and the use of surveillance."

The Chinese government and Communist Party wants to shape a world antithetical to U.S. values and interests and to export its economic, political, and censorship models globally.

In response, the U.S. and like-minded allies must stand resolutely for the freedom of religion, fairer and freer trade, labor rights, freedom of navigation, the rule of law and the freedom of expression—including online.

A coherent and engaged internet freedom strategy must be a critical part of the U.S. diplomatic toolbox. This strategy should have at its core a commitment to protect fundamental freedoms, privacy, and promote the free flow of news and information.

But it is not a matter of just having a strategy, it should be the right one. The Bush and Obama Administrations pursued cyber diplomacy; yet internet freedom has declined around the world, privacy is increasingly under threat, and the free flow of information has become more endangered.

The right strategy must start with some humility. Cyberspace is a place to spread democratic ideals and a place where criminals, extremists, corporations, traffickers, and governments exploit vulnerabilities with impunity. Online

communication can convey are highest ideals and our worst fears. It can shine a light on repression and be the source of hatred, manipulation, fake news, coercion, and conflict. It can bring people together or push us apart.

Despite all this, I agree with the NSS's conclusions which says,

> "The Internet is an American invention, and it should reflect our values as it continues to transform the future for all nations and all generations. A strong, defensible cyber infrastructure fosters economic growth, protects our liberties, and advances our national security."

Central to a revitalized U.S. internet freedom strategy should be a priority to open gaping holes in China's Great Firewall.

Right now, I'm just not confident that this is the policy of the Broadcasting Board of Governors or the State Department right now.

I think there are certain goals we should prioritize in our internet freedom strategy regarding China.

1) China's netizens require easy, reliable and free access to uncensored information through anti-censorship technologies, so that anybody can freely access information regardless of their technical ability. Reliable solutions should work all the time, regardless of intensified crackdowns or major events (Party Congress, June 4th anniversary) taking place in-country.
2) Solutions should also present difficult choices for the Chinese authorities - if the authorities want to disrupt these solutions, then they must disrupt many online services which they would normally be hesitant and unlikely to block.
3) Access to solutions should also come at no cost for Chinese netizens, the Chinese authorities often block access to payment providers so even if Chinese can afford a circumvention solution, they cannot get past censorship by their payment provider.
4) Holistic anti-censorship solutions should be encouraged, including not just technical circumvention but also distribution of those tools (getting around Google Play being blocked, and censorship in the Apple App

Store) and well as helping users share anti-censorship tools, as well as content, through messaging apps, social networks and QR codes.

These are just a few starting principles, I am open to a conversation about these goals with experts and allies. But given the stakes and possible outcomes, moving quickly to fund and distribute anti-censorship technologies should be a priority.

The future safety and prosperity of our grandchildren—in the U.S. and China alike—may very well depend on "open, interoperable communications online, with minimal barriers to the global exchange of information, data, ideas, and services."